CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office, via EFS-Web, on February 14, 2011.

/Wesley L. Austin/

Attorney for Applicants

PATENT APPLICATION
Docket No. AUZ-001 P

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	David M. Austin et al.	
Serial No.:	09/491,727	
Filed:	January 27, 2000	Group Art Unit: 2431
For:	DETECTION OF OBSERVER PROGRAMS AND COUNTERMEASURES AGAINST OBSERVER PROGRAMS	
Examiner:	Syed Zia	

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

An Office Action dated September 14, 2010 (hereinafter, "Office Action") rejected all pending claims (claims 1-6 and 7-18) in the present application. A Notice of Appeal was submitted on December 14, 2010. Appellant's Appeal Brief is being filed herewith.

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest is the assignee, Trapware Corporation.

2. RELATED APPEALS AND INTERFERENCES

An appeal was filed in a continuation-in-part application, Application No. 10/027,714. A Notice of Appeal was filed on July 6, 2006. The Board of Patent Appeals and Interferences decided the appeal on July 28, 2008 affirming the Examiner. Another Notice of Appeal was filed on June 24, 2010. In response to the Notice of Appeal and Appeal Brief, App. No. 10/027,714 was allowed and a Notice of Allowance was mailed on November 3, 2010.

An appeal had been filed in the parent patent application, Application No. 09/491,727. A Notice of Appeal was filed on June 6, 2005. In response to the Notice of Appeal and Appeal Brief, the finality of the last office action on App. No. 09/491,727 was withdrawn and a new office action was mailed on April 21, 2006. Another Notice of Appeal was filed on May 22, 2007. In response to the Notice of Appeal and Appeal Brief a new office action was mailed on November 15, 2007. Another Notice of Appeal was filed on February 15, 2008. An RCE was filed Sep. 16, 2008.

3. STATUS OF CLAIMS

Claims 1-6 and 8-18 are pending in the present application. Claims 7 and 19 have been canceled. Claims 20-32 have been withdrawn from consideration due to a restriction/election requirement. Claim 18 stands rejected under 35 U.S.C. § 101. Claims 1-6 and 8-18 stand rejected under 35 U.S.C. § 103(a) based on Togawa, U.S. Patent No. 6,240,530 (hereinafter, "Togawa"), in view of Drake, U.S. Patent No. 6,006,328 (hereinafter, "Drake") and in further view of Watts, U.S. Patent No. 6,240,530 (hereinafter, "Watts").

Appellants appeal the rejections of claims 1-6 and 8-18.

4. STATUS OF AMENDMENTS

No amendments were filed subsequent to the final rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

As stated in the background section of the patent application, software has been developed to observe or monitor computer users. These software programs provide a wide variety of monitoring features. For example, some of these programs are able to log keystrokes of a user, log menu commands, take screen shots of a user's computer screen at various times, track use of various programs, track what web sites have been visited, monitor e-mail communications, etc. With the technology available today, most, if not all, of a computer user's activities on a computer can be observed and recorded. See the Appellants' patent application (hereinafter referred to as the "Specification"), page 3, lines 1-22.

With the computer technology of today and with the observing programs now available and for those programs that will surely be developed and used in the future, computer users may be watched by third parties more often than many think. It would be highly beneficial to computer users if they could find out whether they are being observed by computer software and technology and to know information about the observing activity and/or program. Specification, page 3, lines 1-22.

As presently claimed, a new system has been developed for detecting an observing program on a computer system as including accessing instructions that access observer data. One or more embodiments of an observer program are described in the Specification on page 14, lines 9-23, page 15, lines 1-14, and Figure 2. The observer data includes data descriptive of the observer program. The observer program is programmed to observe a user's activities on the computer system and also operates to create data from its observations. The system also includes reading instructions that read memory of the computer system to obtain memory data. Further, the system includes comparing instructions that compare the observer data with memory data read in from memory to determine whether the observer program is present on the computer system. One or more embodiments of the system and how it detects an observer program are described in the Specification on page 17, lines 8-22, page 18, lines 1-23, page 19, lines 1-23, page 20, lines 1-23, page 21, lines 1-23, 9-23, and Figure 3. The system also includes generating instructions that generate results from the reading and comparing. The results generated indicate whether the observer program is present on the computer system. In addition, the system includes outputting instructions that obtain the results and provide the results for a user. The outputting instructions may provide the results to a user through a graphical user interface.

As required by 37 C.F.R. § 41.37(c)(1)(v), a summary of claimed subject matter immediately follows. The references to the specification refer only to embodiments of the invention. The invention is defined by the claims. Accordingly, these references to the specification are not meant to limit the scope of the claims of the present invention in any way but are only provided because they are mandated by 37 C.F.R. § 41.37(c)(1)(v). All references are to the patent specification.

1. A system for detecting the presence of an observing program on a computer system, the system comprising:

a computer system comprising a processor, memory, a user input device and a monitor,

wherein the memory comprises:

observer data that includes data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system by monitoring user input entered through a user input device and also operating to create a log file from the observing of the observer program; (pg. 9, lines 6-8; pg. 10, lines 4-15; pg. 14, lines 9-23; pg. 15, lines 1-23; pg. 16, lines 1-23; pg. 17, lines 1-7; Figure 2, elements 34-48; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23)

accessing instructions that access the observer data; (pg. 9, lines 5-6; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 17, lines 8-23; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

reading instructions that read the memory of the computer system to obtain memory data; (pg. 9, lines 8-10; pg. 10, lines 16-23; pg. 11, lines 1-8; pg, 11, lines 9-18; pg. 17, lines 8-23; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

comparing instructions that compare the observer data with memory data read in from the memory to determine whether the observer program is present on the computer system; (pg. 9, lines 10-12, 15-24; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

generating instructions that generate results from the comparing, wherein the results generated indicate whether the observer program is present on the computer system; (pg. 9, lines 12-15, 15-24; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 22, lines 5-11; Figure 4; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

countermeasure instructions that alter the operation of the observer program; (pg. 22, lines 12-23; pg. 28, lines 11-23; pg. 29, lines 1-23; pg. 30, lines 1-23; pg. 31, lines 1-22; Figure 4, Figure 7, Figure 8 and Figure 9)

outputting instructions that obtain the results and provide the results for a user and that prompt the user as to whether the countermeasure instructions should be executed. (pg. 10, lines 1-3; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 22, lines 5-11; Figure 4; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

16. A system for detecting the presence of an observing program on a computer system, the system comprising:

a computer system comprising a processor, memory, a user input device and a monitor, wherein the memory comprises:

observer data that includes data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system by monitoring user input entered through a user input device and also operating to create a log file from the observing of the observer program; (pg.

9, lines 6-8; pg. 10, lines 4-15; pg. 14, lines 9-23; pg. 15, lines 1-23; pg. 16, lines 1-23; pg. 17, lines 1-7; Figure 2, elements 34-48; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23)

means for accessing the observer data; (pg. 9, lines 5-6; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 17, lines 8-23; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

means for reading the memory of the computer system to obtain memory data; (pg. 9, lines 8-10; pg. 10, lines 16-23; pg. 11, lines 1-8; pg, 11, lines 9-18; pg. 17, lines 8-23; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

means for comparing the observer data with memory data to determine whether the observer program is present on the computer system; (pg. 9, lines 10-12, 15-24; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

means for generating results from the comparison, wherein the results generated indicate whether the observer program is present on the computer system; (pg. 9, lines 12-15, 15-24; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 22, lines 5-11; Figure 4; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

means for altering the operation of the observer program; and (pg. 22, lines 12-23; pg. 28, lines 11-23; pg. 29, lines 1-23; pg. 30, lines 1-23; pg. 31, lines 1-22; Figure 4, Figure 7, Figure 8 and Figure 9)

means for outputting the results for a user and for prompting the user as to whether the countermeasure instructions should be executed. (pg. 10, lines 1-3; pg.

10, lines 16-23; pg. 11, lines 1-8; pg. 22, lines 5-11; Figure 4; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

17. A method for detecting the presence of an observing program on a computer system, wherein the observing program is programmed to observe a user's activities on the computer system by monitoring user input entered through a user input device and to create data from the observing on the computer system, the method being implemented through computer software for running on the computer system, the method comprising the steps of:

accessing observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system by monitoring user input entered through a user input device and also operating to create a log file from the observing of the observer program; (pg. 9, lines 5-6; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 17, lines 8-23; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

reading memory of the computer system to obtain memory data; (pg. 9, lines 8-10; pg. 10, lines 16-23; pg. 11, lines 1-8; pg, 11, lines 9-18; pg. 17, lines 8-23; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

comparing the observer data with memory data read in from memory to determine whether the observer program is present on the computer system; (pg. 9, lines 10-12, 15-24; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

generating results from the reading and comparing, wherein the results generated indicate whether the observer program is present on the computer system; (pg. 9, lines 12-15,

15-24; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 22, lines 5-11; Figure 4; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

outputting the results for a user; and (pg. 10, lines 1-3; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 22, lines 5-11; Figure 4; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

prompting the user as to whether countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running. (pg. 22, lines 12-23; pg. 28, lines 11-23; pg. 29, lines 1-23; pg. 30, lines 1-23; pg. 31, lines 1-22; Figure 4, Figure 7, Figure 8 and Figure 9)

18. An article of manufacture comprising:

a tangible computer-readable storage medium containing instructions for detecting the presence of an observing program on a computer system, wherein the instructions are executable to:

access observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system by monitoring user input entered through a user input device and also operating to create a log file from the observing of the observer program; (pg. 9, lines 5-6; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 17, lines 8-23; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

read memory of the computer system to obtain memory data; (pg. 9, lines 8-10; pg. 10, lines 16-23; pg. 11, lines 1-8; pg, 11, lines 9-18; pg. 17, lines 8-23; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

compare the observer data with memory data read in from memory to determine whether the observer program is present on the computer system; (pg. 9, lines 10-12, 15-24; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 18, lines 1-23; pg. 19, lines 1-23; pg. 20, lines 1-23; pg. 21, lines 1-23; Figure 3, elements 50-60; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

generate results from the read and compare, wherein the results generated indicate whether the observer program is present on the computer system; (pg. 9, lines 12-15, 15-24; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 22, lines 5-11; Figure 4; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

output the results for a user; and (pg. 10, lines 1-3; pg. 10, lines 16-23; pg. 11, lines 1-8; pg. 22, lines 5-11; Figure 4; pg. 23, lines 5-23; pg. 24, lines 1-23; pg. 25, lines 1-23; pg. 26, lines 1-23; pg. 27, lines 1-23; Figure 5; Figure 6)

prompt the user as to whether countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running. (pg. 22, lines 12-23; pg. 28, lines 11-23; pg. 29, lines 1-23; pg. 30, lines 1-23; pg. 31, lines 1-22; Figure 4, Figure 7, Figure 8 and Figure 9)

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following issues are presented for review:

A. Whether claim 18 is unpatentable under 35 U.S.C. § 101;

B. Whether claims 1-6 and 8-18 are unpatentable under 35 U.S.C. § 103(a) based on Togawa in view of Drake in view of Watts.

7. ARGUMENT

A. Claim 18 Rejected Under 35 U.S.C. § 101

Claim 18 stands rejected under 35 U.S.C. § 101. Claim 18 recites "[a]n article of manufacture comprising: a ***tangible*** computer-readable ***storage*** medium containing . . ." (emphasis added.) Thus, claim 18 is limited to only physical, non-transitory storage media.

B. Claims 1-6 and 8-18 Rejected Under 35 U.S.C. § 103(a)

The Examiner rejected claims 1-6 and 8-18 stand rejected under 35 U.S.C. § 103(a) based on Togawa, U.S. Patent No. 6,240,530 (hereinafter, "Togawa"), in view of Drake, U.S. Patent No. 6,006,328 (hereinafter, "Drake") and in further view of Watts, U.S. Patent No. 6,240,530 (hereinafter, "Watts").The M.P.E.P. states that

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure.
>
> The initial burden is on the examiner to provide some suggestion of the desirability of doing what the inventor has done. To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references.

M.P.E.P. § 2142.

Appellants respectfully submit that the claims at issue are patentably distinct from the cited references.

Rejection of Claims 1-6, 8, 10-18

Claim 1 recites "countermeasure instructions that alter the operation of the observer program." Towaga, alone or in combination with Drake and Watts, does not teach or suggest this subject matter. Instead Towaga states:

> According to a further aspect of the present invention, there is provided an information processing apparatus which includes a memory for storing programs and data for information processing and a processing section for executing the programs to perform various information processing, comprising a virus detection and identification section for detecting a computer virus which infects the information processing apparatus and identifying a type of the detected computer virus, a virus type information registration section for registering information regarding the type of the detected computer virus identified by the virus detection and identification section into a storage area which is access-disabled in an ordinary operation of the information processing apparatus, a trigger information outputting section for outputting trigger information so that the information processing apparatus may enter a processing mode for performing virus extermination, a stored information clearing section operable in response to the trigger information from the trigger information outputting section for clearing information stored in all of those areas of the memory which are access-enabled in an ordinary operation of the information processing apparatus, an operating system fetching and starting up section for fetching an operating system from the outside and starting up the operating system after the stored information is cleared by the stored information clearing section, and a virus extermination section for exterminating, in operation environment of the operating system started up by the operating system fetching and starting up section, the computer virus which infects the memory of the information processing apparatus based on the information regarding the type of the detected virus registered in the virus type information storage section.

Togawa, col. 5, lines 7-38. This portion of Togawa does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

Togawa also states:

> FIG. 1 illustrates in flow chart a virus extermination method according to an aspect of the present invention. Referring to FIG. 1. the virus extermination method illustrated includes a virus detection and identification step S1, a memory clearing step S3, an operating system fetching and starting up step S4 and a virus extermination step S5 in order

> to exterminate a computer virus as a software destroying factor which infects a computer system.
>
> More particularly, in the virus detection and identification step S1, a computer virus as a software destroying factor which infects a computer system is detected and a type of the computer virus is identified. If such an infecting computer virus is detected in the virus detection and identification step S1 (the YES route of step S2), then information stored in all of those areas of a memory which are in a write-enabled state in an ordinary operation of the computer system is cleared in the memory clearing step S3.

Togawa, col. 8, lines 14-30. This portion of Togawa does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

The addition of Drake does not overcome the deficiencies of Togawa. Instead Drake states:

> The improved process consists of including computer code to automatically detect tampering of said computer software, and computer code to prevent the theft of ID-Data by replacing existing vulnerable (to rogue software eavesdropping or attack) software or operating system code with secure equivalents which utilise anti-spy techniques (as described later in this document).

Drake, col. 3, lines 38-44. This portion of Drake does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

Drake also states:

> This can be achieved with the use of code which is protected from disassembly and examination through obfuscation and encryption, which re-reads its own external-image and compares it with its known memory image or precalculated check-data to detect hot-patching (ie. the modification of software sometime after it has been loaded from disk, but (usually) before execution of the modified section has commenced).
>
> Additionally, the software can scan the memory image of itself one or more times, or continuously, to ensure that unexpected alterations do not occur.

Drake, col. 6, lines 10-20. This portion of Drake does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

The addition of Watts does not overcome the deficiencies of Togawa and Drake. Instead Watts states:

> Function of detecting a computer virus as a software-detroying factor which infects a computer system and identifying a type of the computer virus, a memory clearing function of receiving trigger information . . .

Watts, col. 6, lines 10-12. This portion of Watts does not teach or suggest "countermeasure instructions that alter the operation of the observer program."

Claim 1 also recites "outputting instructions that obtain the results and provide the results for a user and that prompt the user as to whether the countermeasure instructions should be executed." Towaga, alone or in combination with Drake and Watts, does not teach or suggest this subject matter. Instead Togawa states:

> According to a further aspect of the present invention, there is provided an information processing apparatus which includes a memory for storing programs and data for information processing and a processing section for executing the programs to perform various information processing, comprising a virus detection and identification section for detecting a computer virus which infects the information processing apparatus and identifying a type of the detected computer virus, a virus type information registration section for registering information regarding the type of the detected computer virus identified by the virus detection and identification section into a storage area which is access-disabled in an ordinary operation of the information processing apparatus, a trigger information outputting section for outputting trigger information so that the information processing apparatus may enter a processing mode for performing virus extermination, a stored information clearing section operable in response to the trigger information from the trigger information outputting section for clearing information stored in all of those areas of the memory which are access-enabled in an ordinary operation of the information processing apparatus, an operating system fetching and starting up section for fetching an operating system from the outside and starting up the operating system after the stored information is cleared by the stored information clearing section, and a virus extermination section for exterminating, in operation environment of the operating system started up by the operating system fetching and starting up section, the computer virus which infects the memory of the information processing apparatus based on the information regarding the type of the detected virus registered in the virus type information storage section.

Togawa, col. 5, lines 7-38. This portion of Togawa does not teach or suggest "outputting instructions . . . that prompt the user as to whether the countermeasure instructions should be executed."

Togawa also states:

> FIG. 1 illustrates in flow chart a virus extermination method according to an aspect of the present invention. Referring to FIG. 1. the virus extermination method illustrated includes a virus detection and identification step S1, a memory clearing step S3, an operating system fetching and starting up step S4 and a virus extermination step S5 in order to exterminate a computer virus as a software destroying factor which infects a computer system.
>
> More particularly, in the virus detection and identification step S1, a computer virus as a software destroying factor which infects a computer system is detected and a type of the computer virus is identified. If such an infecting computer virus is detected in the virus detection and identification step S1 (the YES route of step S2), then information stored in all of those areas of a memory which are in a write-enabled state in an ordinary operation of the computer system is cleared in the memory clearing step S3.

Togawa, col. 8, lines 14-30. This portion of Togawa does not teach or suggest "outputting instructions . . . that prompt the user as to whether the countermeasure instructions should be executed."

The addition of Drake does not overcome the deficiencies of Togawa. Instead Drake states:

> The improved process consists of including computer code to automatically detect tampering of said computer software, and computer code to prevent the theft of ID-Data by replacing existing vulnerable (to rogue software eavesdropping or attack) software or operating system code with secure equivalents which utilise anti-spy techniques (as described later in this document).

Drake, col. 3, lines 38-44. This portion of Drake does not teach or suggest "outputting instructions that obtain the results and provide the results for a user and that prompt the user as to whether the countermeasure instructions should be executed."

Drake also states:

> This can be achieved with the use of code which is protected from disassembly and examination through obfuscation and encryption, which re-reads its own external-image and compares it with its known memory

> image or precalculated check-data to detect hot-patching (ie. the modification of software sometime after it has been loaded from disk, but (usually) before execution of the modified section has commenced).
>
> Additionally, the software can scan the memory image of itself one or more times, or continuously, to ensure that unexpected alterations do not occur.

Drake, col. 6, lines 10-20. This portion of Drake does not teach or suggest "outputting instructions that obtain the results and provide the results for a user and that prompt the user as to whether the countermeasure instructions should be executed."

The addition of Watts does not overcome the deficiencies of Togawa and Drake. Instead Watts states:

> Function of detecting a computer virus as a software-detroying factor which infects a computer system and identifying a type of the computer virus, a memory clearing function of receiving trigger information . . .

Watts, col. 6, lines 10-12. This portion of Watts does not teach or suggest "outputting instructions that obtain the results and provide the results for a user and that prompt the user as to whether the countermeasure instructions should be executed."

In view of the foregoing, Applicants respectfully submit that claim 1 is patentably distinct from the cited references. Accordingly, Applicants respectfully request that the rejection of claim 1 be withdrawn because Towaga, alone or in combination with Drake and Watts, does not teach or suggest all of the subject matter of claim 1.

Claims 2-15 depend either directly or indirectly from claim 1. Accordingly, Applicants respectfully request that the rejection of claims 2-15 be withdrawn.

Claim 16 recites "means for altering the operation of the observer program; and means for outputting the results for a user and for prompting the user as to whether the countermeasure instructions should be executed." As discussed above, Towaga, alone or in combination with Drake and Watts, does not teach or suggest this claimed subject matter. Accordingly, Applicants respectfully submit that claim 16 is allowable.

Claim 17 recites "prompting the user as to whether countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running." As discussed above,

Towaga, alone or in combination with Drake and Watts, does not teach or suggest this claimed subject matter. Accordingly, Applicants respectfully submit that claim 17 is allowable.

Claim 18 recites "prompt the user as to whether countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running." As discussed above, Towaga, alone or in combination with Drake and Watts, does not teach or suggest this claimed subject matter. Accordingly, Applicants respectfully submit that claim 18 is allowable.

Rejection of Claim 9

Claim 9 should be allowed for the reasons as set forth above. In addition to the foregoing reasons, claim 9 is allowable over the prior art because none of the references teach or suggest "wherein the countermeasure instructions alter the operation of the observer program by altering a file on the computer system, and wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running." Thus claim 9 requires that the countermeasure instructions are executable to perform the following three functions: "(1) temporarily disable the observer program, (2) permanently disable the observer program, ***and*** (3) create decoy observer created data but wherein the observer program continues running" (emphasis added). Neither Drake nor Togawa, as suggested by the Office Action, teaches or suggests countermeasure instructions that perform the three functions recited. Togawa may teach detecting and exterminating a virus, but this falls far short of teaching and suggesting the claim limitations of claim 9. Additionally, Drake may teach detect tampering and keeping the detection of tampering secret, but this does not teach or suggest the claim limitations as required by claim 9. Accordingly, Applicants respectfully submit that claim 9 is allowable.

Respectfully submitted,

/Wesley L. Austin/

Wesley L. Austin
Reg. No. 42,273
Attorney for Appellant(s)

Date: February 14, 2011

AUSTIN RAPP & HARDMAN
170 South Main Street, Suite 735
Salt Lake City, UT 84101
Telephone: (801) 537-1700

CLAIMS APPENDIX

Listing of Claims involved in the appeal:

1. A system for detecting the presence of an observing program on a computer system, the system comprising:

a computer system comprising a processor, memory, a user input device and a monitor,

wherein the memory comprises:

observer data that includes data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system by monitoring user input entered through a user input device and also operating to create a log file from the observing of the observer program;

accessing instructions that access the observer data;

reading instructions that read the memory of the computer system to obtain memory data;

comparing instructions that compare the observer data with memory data read in from the memory to determine whether the observer program is present on the computer system;

generating instructions that generate results from the comparing, wherein the results generated indicate whether the observer program is present on the computer system;

countermeasure instructions that alter the operation of the observer program; and

outputting instructions that obtain the results and provide the results for a user and that prompt the user as to whether the countermeasure instructions should be executed.

2. The system of claim 1 wherein the reading instructions read the memory of the computer system by querying the operating system of the computer system for the tasks running and by examining task information provided by the operating system.

3. The system of claim 1 wherein the outputting instructions provide the results to a user through a graphical user interface.

4. The system of claim 1 wherein the reading instructions read the memory of the computer system by querying the file system of the computer system for the files located on storage media and by examining file information provided by the file system.

5. The system of claim 1 wherein the reading instructions read the memory of the computer system by opening a file located on storage media and by examining contents of the file.

6. The system of claim 1 wherein the observer data includes data descriptive of a plurality of observer programs and wherein the system compares the observer data with the memory data to determine whether any known observer program is present.

7. (Canceled)

8. The system of claim 1 wherein the countermeasure instructions alter the operation of the observer program by altering observer program configuration data.

9. The system of claim 1 wherein the countermeasure instructions alter the operation of the observer program by altering a file on the computer system, and wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running.

10. The system of claim 1 wherein the countermeasure instructions alter the operation of the observer program by altering reporting data generated by the observer program.

11. The system of claim 1 wherein the countermeasure instructions alter the operation of the observer program by replacing reporting data generated by the observer program but wherein the observer program continues running.

12. The system of claim 1 wherein the countermeasure instructions alter the operation of the observer program by replacing a file of the observer program.

13. The system of claim 1 wherein the observer data includes data descriptive of observing activity typical of observing programs and wherein the system compares the observer data with the memory data to determine whether any known observer program is present.

14. The system of claim 1 further comprising the observer data, wherein the observer data includes a list of files and modules that are part of the observer program software, and wherein the reading instructions read the memory of the computer system by querying the operating system of the computer system for the tasks running and by examining task information provided by the operating system, and wherein the reading instructions also read the memory of the computer system by querying the file system of the computer system for the files located on storage media and by examining file information provided by the file system, and wherein the outputting instructions provide the results to a user through a graphical user interface.

15. The system of claim 1 wherein the system is made available over a computer network through a web site.

16. A system for detecting the presence of an observing program on a computer system, the system comprising:

a computer system comprising a processor, memory, a user input device and a monitor,

wherein the memory comprises:

observer data that includes data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system by monitoring user input entered through a user input device and also operating to create a log file from the observing of the observer program;

means for accessing the observer data;

means for reading the memory of the computer system to obtain memory data;

means for comparing the observer data with memory data to determine whether the observer program is present on the computer system;

means for generating results from the comparison, wherein the results generated indicate whether the observer program is present on the computer system;

means for altering the operation of the observer program; and

means for outputting the results for a user and for prompting the user as to whether the countermeasure instructions should be executed.

17. A method for detecting the presence of an observing program on a computer system, wherein the observing program is programmed to observe a user's activities on the computer system by monitoring user input entered through a user input device and to create data from the observing on the computer system, the method being implemented through computer software for running on the computer system, the method comprising the steps of:

accessing observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system by monitoring user input entered through a user input device and also operating to create a log file from the observing of the observer program;

reading memory of the computer system to obtain memory data;

comparing the observer data with memory data read in from memory to determine whether the observer program is present on the computer system;

generating results from the reading and comparing, wherein the results generated indicate whether the observer program is present on the computer system;

outputting the results for a user; and

prompting the user as to whether countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running.

18. An article of manufacture comprising:

a tangible computer-readable storage medium containing instructions for detecting the presence of an observing program on a computer system, wherein the instructions are executable to:

access observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system by monitoring user input entered through a user input device and also operating to create a log file from the observing of the observer program;

read memory of the computer system to obtain memory data;

compare the observer data with memory data read in from memory to determine whether the observer program is present on the computer system;

generate results from the read and compare, wherein the results generated indicate whether the observer program is present on the computer system;

output the results for a user; and

prompt the user as to whether countermeasure instructions should be executed, wherein the countermeasure instructions are executable to (1) temporarily disable the observer program, (2) permanently disable the observer program, and (3) create decoy observer created data but wherein the observer program continues running.

19. (Cancelled)

20-32. (Withdrawn)

EVIDENCE APPENDIX

NONE.

RELATED PROCEEDINGS APPENDIX

NONE.